Judge Robert S. Lasnik

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff v. SEBASTIEN RAOULT Defendant.	NO. CR21-109 RSL UNITED STATES' SENTENCING MEMORANDUM

Sebastien Raoult played a major role in the sophisticated ShinyHunters hacking scheme, a for-profit international hacking conspiracy that caused millions of dollars in harm to U.S. companies and exposed hundreds of millions of individuals to identity theft. Raoult was instrumental in developing the software code that he and his co-conspirators used for hacking, and he also hacked companies directly. By selling stolen data on dark web forums and through various other means, Raoult and his co-conspirators in the ShinyHunters group profited substantially. Raoult hacked for the purpose of personal profit, and he displayed complete disregard for the harm that he knew people were likely to suffer when buyers of stolen data used customers' financial information. For at least two years, Raoult engaged in hacking for profit, both through the ShinyHunters scheme and through other hacking activities.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Pursuant to a plea agreement, Raoult has pled guilty to conspiracy to commit wire fraud, in violation of 18 U.S.C. § 1349, and aggravated identity theft, in violation of 18 U.S.C. § 1028A. To address Raoult's extremely serious conduct and to deter Raoult and others from engaging in such destructive hacking activity, while also accounting for mitigating factors in Raoult's background, the United States respectfully recommends that the Court impose a custodial sentence of 72 months, to be followed by a 3-year term of supervised release, order restitution in the amount of $5,058,419.73, and impose a mandatory special assessment of $200.

I. BACKGROUND

A. Overview of the Hacking Scheme

Raoult played a major role in a sophisticated hacking scheme. Between April 2020 and June 2021, Raoult conspired with co-defendants Gabriel Bildstein and Abdel-Hakim El Ahmadi and other co-conspirators to hack numerous companies' computers. PSR ¶ 22. Often Raoult and his co-conspirators breached companies by using phishing emails to deceive recipients into disclosing login credentials for accounts at Provider-1, a U.S.-based computer code hosting and development platform. PSR ¶¶ 12, 14; Plea ¶ 9, ECF No. 50. From the victim companies, the hackers stole confidential information and customer records, which contained personally identifiable information and financial information. PSR ¶ 30; Plea ¶ 9. Victim companies suffered millions of dollars in losses. PSR ¶ 30; Plea ¶ 9. The hackers profited handsomely by selling stolen data on dark web forums and demanding ransoms. PSR ¶ 26; Plea ¶ 9.

Raoult developed a substantial portion of the software code and phishing websites that he and his-conspirators used to breach victim companies, as discussed further below. PSR ¶ 22; Plea ¶ 9. In addition, Raoult personally hacked companies in furtherance of the conspiracy. PSR ¶ 25; Plea ¶ 9. He has admitted that he conspired with Bildstein, El Ahmadi, and others in the charged conspiracy beginning by April 1, 2020, and continuing through at least the end of June 2020. Plea ¶ 9. He has also admitted that he continued to

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

conduct computer hacking activities with some of the same co-conspirators, including hacking companies through their employees' accounts at Provider-1, between July 2020 and at least June 2021. Plea ¶ 9.

One of the conspirators' most common attack vectors involved sending phishing emails to dupe recipients into disclosing access credentials, especially for accounts at Provider-1. PSR ¶ 14; Plea ¶ 9. Raoult and his co-conspirators used false names and addresses to register domain names for websites that spoofed the login pages of legitimate providers, such as Provider-1. PSR ¶ 16; Plea ¶ 9. They sent phishing emails to company employees that purported to come from Provider-1. PSR ¶ 15; Plea ¶ 9. Those emails instructed the recipients to click on a link, which directed the recipient to one of the fake login pages to enter their access credentials, such as username and password. PSR ¶ 15; Plea ¶ 9.

Using the stolen usernames and passwords, Raoult and his co-conspirators accessed victim employees' accounts at Provider-1 and other service providers. PSR ¶¶ 15, 17-18; Plea ¶ 9. If victim employees had two-factor authentication set up, the phishing websites prompted them to provide their authentication code. PSR ¶ 15; Plea ¶ 9. Raoult and his co-conspirators not only stole the data from the initial breached accounts, such as the contents of code repositories at Provider-1, but also searched those accounts for credentials to companies' networks and other third-party service providers, such as cloud storage services. PSR ¶ 18; Plea ¶ 9. The hackers used those additional stolen credentials to further breach the victim companies. PSR ¶ 18; Plea ¶ 9.

Raoult bragged about the key role that he played in developing the software code for the group's hacking activities. Provider-1 had recognized the hacking campaign and dubbed it "Sawfish," a term that then also appeared in media articles. In a Discord conversation using his account Sezyo#1234, Raoult spoke proudly about how he had designed the scam:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Sezyo#1234	Still, my greatest success as dark haxor was sawfish	2021-03-14 18:03:43 UTC
Sezyo#1234	When I see the articles	2021-03-14 18:03:53 UTC
Sezyo#1234	It's great	2021-03-14 18:03:58 UTC
Liebert#3914	Sawfish?	2021-03-14 18:04:25 UTC
Sezyo#1234	The [Provider-1] phishing during the first lockdown	2021-03-14 18:04:38 UTC
Sezyo#1234	With my spectacular scam that clones automatically	2021-03-14 18:04:50 UTC

SH-00116864 – 00116865 (translation from French).

Technical evidence confirms Raoult's key role in developing the software code and phishing websites that he and his co-conspirators in the ShinyHunters group used to breach victim companies, especially through Provider-1. For example, Raoult maintained his own account at Provider-1 with the username Sezyokzn. PSR ¶ 22; Plea ¶ 9. Records from that account show that Raoult used it to test numerous phishing websites that spoofed Provider-1's login page. PSR ¶ 22; Plea ¶ 9. Raoult also used Discord to share and discuss software code for the scheme with his co-conspirators. PSR ¶¶ 23-24; *See, e.g.*, SH-00116947 – 00117031.

French law enforcement interviewed Raoult's co-conspirator, Bildstein, who also confirmed Raoult's important role in the conspirators' campaign to hack companies through accounts at Provider-1. When they asked Bildstein, "[W]ho was responsible for the phishing used to get the accounts on [Provider-1]?," Bildstein responded, "It was Abdel and Sezyo mainly who were responsible . . . ." SH-00119530 (translation from French). In response to the question, "What was this phishing operation called SAWFISH?." Bildstein explained, "It was Abdel's idea . . . the scripts were coded by Sezyo . . . ." SH-00119526. In addition, "Sezyo had coded a BOT on Discord to see the results live when they arrived and at least 3 people at a time monitored the results to siphon it when it arrived." SH-00119526. Monitoring the results was important because

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

"[w]e recovered the two-factor authentication code and we had to enter it quickly before the legitimate user did." SH-00119534. Bildstein also described "Shinyhunters crypto hacks organized by Sebastien." SH-00119522. According to Bildstein, Raoult was "the speaker of the group who talked to everyone." SH-00119522.[1]

In addition to developing the software code and phishing websites, Raoult personally participated in hacking victims. PSR ¶ 25; Plea ¶ 9. For example, Raoult used stolen access credentials belonging to an employee of Victim-2, a U.S.-based media and entertainment company, to breach that employee's account at Provider-1 and thereby steal confidential data belonging to Victim-2. PSR ¶ 25; Plea ¶ 9. In furtherance of the conspiracy, Raoult and his co-conspirators hacked numerous companies, including companies in the Western District of Washington, elsewhere in the United States, and in other countries, as described further below. PSR ¶ 11; Plea ¶ 9.

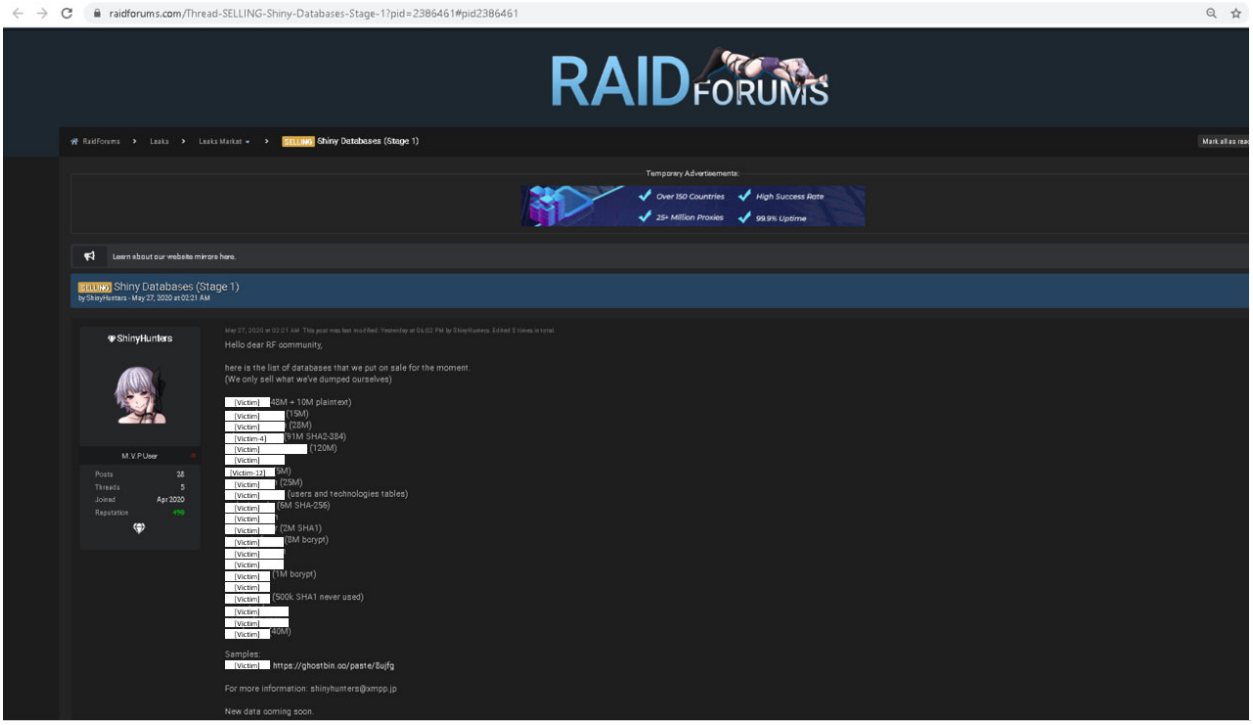
B. The Hacking Scheme Generated Substantial Profits

After Raoult and his co-conspirators hacked companies, a user going by the name ShinyHunters posted hacked data from many of those companies for sale on dark web marketplaces, including RaidForums, EmpireMarket, and Exploit. PSR ¶¶ 19, 26; Plea ¶ 9. A company's stolen data typically sold for thousands of dollars, and ShinyHunters sometimes sold the same company's data multiple times. PSR ¶ 26; Plea ¶ 9. Between April 2020 and June 2021, ShinyHunters posted sales of hacked data from more than 60 companies. PSR ¶ 26; Plea ¶ 9. For example, as of May 18, 2020, ShinyHunters had 12 databases available for sale on Empire Market. SH-00114465. In a single post on

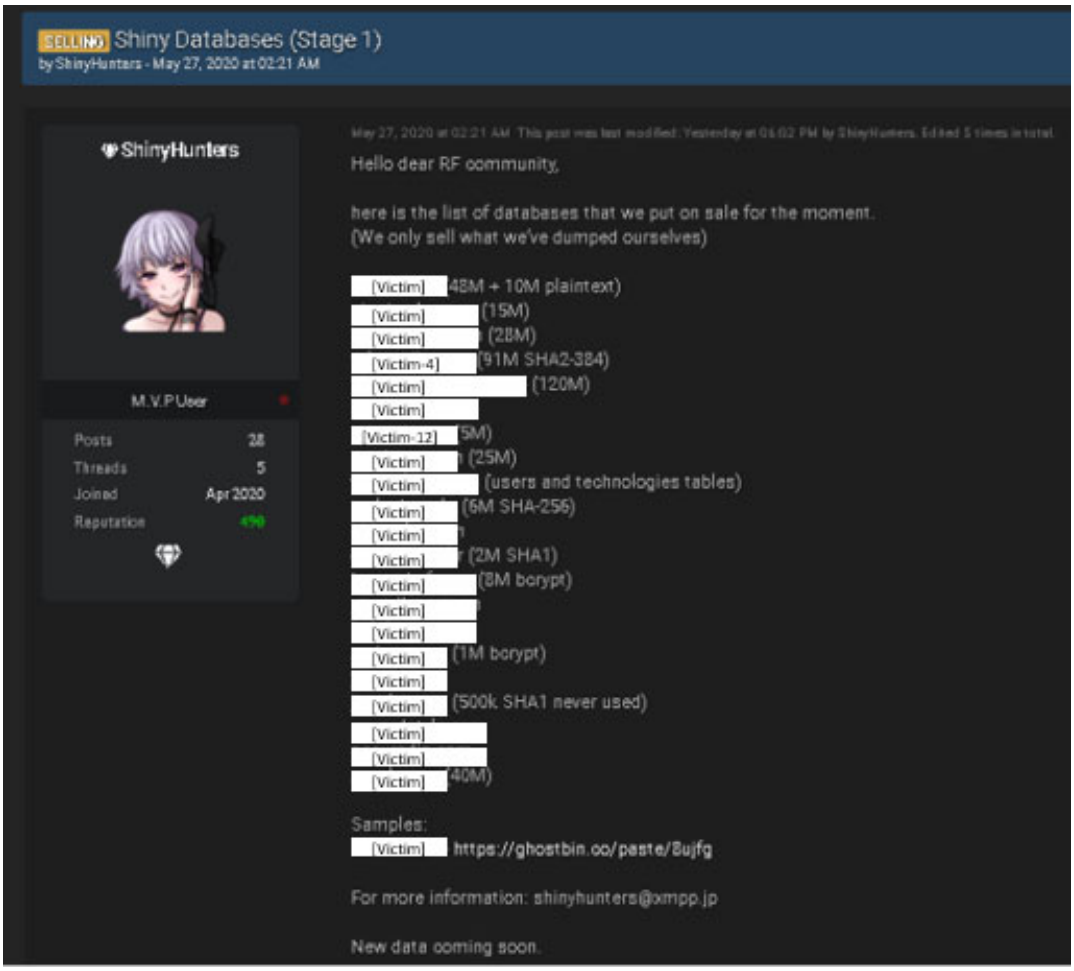
[1] Regarding Raoult, Bildstein also stated, "he is less implicated in Shinyhunters. He took care of 'credential stuffing' on [Provider-1] and once he succeeded, he asked me to do the rest because he didn't have the skills to do it. Then, we shared the profits for the sake of fairness . . . ." SH-00119519. Credential stuffing is a method for using stolen credentials to breach accounts. Bildstein appears to have been saying that Raoult was primarily responsible for the initial stage of the attack that breached a victim's account at Provider-1, but that Raoult was less involved in later stages of exfiltrating data from additional sources, such as cloud service providers. Bildstein may also have been suggesting that Raoult was less involved in other ShinyHunters activity that was not based on breaching Provider-1 accounts. Since most of the victims at issue in this case were breached through the Sawfish phishing attacks on Provider-1 accounts, there is no ambiguity that Raoult was instrumental in that hacking activity.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

RaidForums on May 27, 2020, ShinyHunters made 21 companies' databases available for sale, as shown below (with victims' names redacted for privacy). PSR ¶ 19. The first image shows the full screen version of the post, and the second image expands the key text for readability:



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970



SH-00002306. In this post, ShinyHunters told viewers, "We only sell what we've dumped ourselves," and "New data coming soon." In addition to identifying the victim names, ShinyHunters provided the number of associated customer records in millions for most of the victims. This and other posts also directed potential buyers to contact ShinyHunters at the account shinyhunters@xmpp.jp.

For example, ShinyHunters posted the stolen data from Victim-4 for sale on RaidForums and Empire Market in May 2020. SH-00002306, SH-00114465. Both posts advertised that the data included 91 million customer records. On Empire Market, ShinyHunters listed that the sale price was $5,000. SH-00114465. Numerous interested buyers contacted shinyhunters@xmpp.jp. SH-00116287. As of May 5, 2020, shinyhunters@xmpp.jp stated that Victim-4's data had been sold a total of 13 times so

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

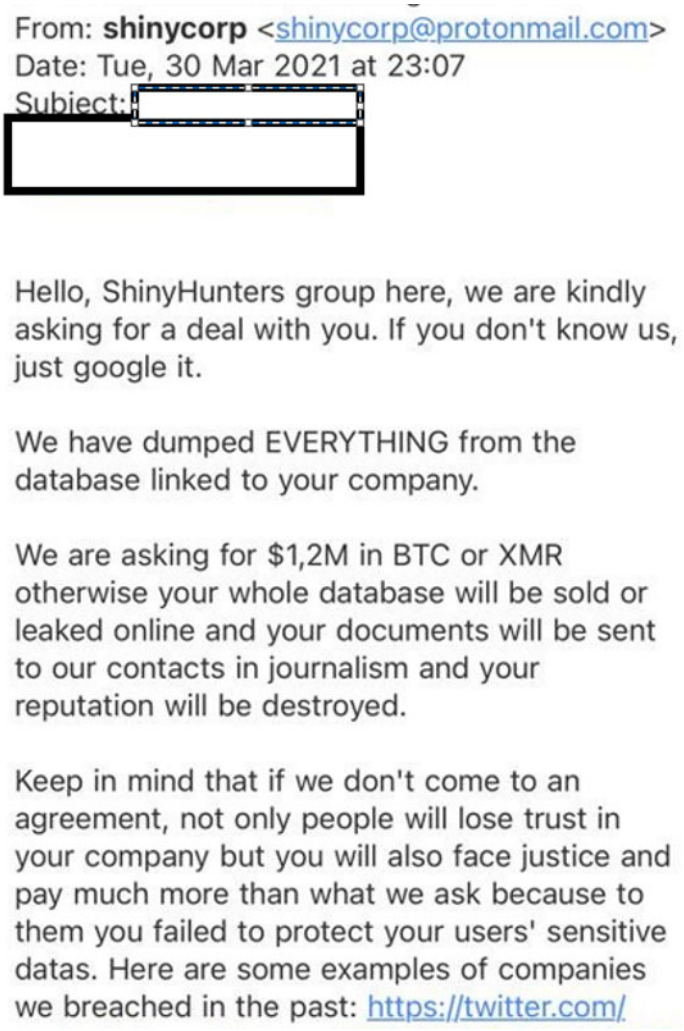
far. SH-00116287. Thus, ShinyHunters collected at least $65,000 from the sales of Victim-4's stolen data. PSR ¶ 26; Plea ¶ 9. Raoult discussed the sale of Victim-4's data with Bildstein in messages found on one of Bildstein's devices. PSR ¶ 26. On May 8, 2020, using the account unweakrvl@jabber.ua, Raoult asked Bildstein about how the sale of Victim-4's data was going:

unweakrvl@jabber.ua 2020-05-08T14:25:33+0200	on [Victim-4] , did you manage to sell it well?
unweakrvl@jabber.ua 2020-05-08T14:26:20+0200	me too I want to sell databases if I don't get into crypto sites because the wallet does not work at all there
allgodschildren@jabber.ua 2020-05-08T14:26:39+0200	yes, right
unweakrvl@jabber.ua 2020-05-08T14:27:17+0200	need to redo a [Provider-1] spam, but I think we have to change the scama/malware so it doesn't get detected quickly

SH-00119339 (translation from French); PSR ¶ 26; Plea ¶ 9.

In addition to selling stolen data, ShinyHunters also demanded ransoms from some victims in return for not disseminating the stolen data. PSR ¶ 26; Plea ¶ 9. ShinyHunters succeeded in obtaining ransoms as large as $425,000. PSR ¶ 26; Plea ¶ 9. For example, one victim paid a ransom of $15,000 in May 2020. SH-00076906. In another example, in March 2021, ShinyHunters demanded a ransom of $1.2 million in bitcoin from a victim:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970



From: **shinycorp** <shinycorp@protonmail.com>
Date: Tue, 30 Mar 2021 at 23:07
Subject: [redacted]

Hello, ShinyHunters group here, we are kindly asking for a deal with you. If you don't know us, just google it.

We have dumped EVERYTHING from the database linked to your company.

We are asking for $1,2M in BTC or XMR otherwise your whole database will be sold or leaked online and your documents will be sent to our contacts in journalism and your reputation will be destroyed.

Keep in mind that if we don't come to an agreement, not only people will lose trust in your company but you will also face justice and pay much more than what we ask because to them you failed to protect your users' sensitive datas. Here are some examples of companies we breached in the past: https://twitter.com/

SH-00004058; PSR ¶ 20. Based on tracing bitcoin payments, ShinyHunters appears to have actually received a ransom of approximately $425,000. SH-00114438.

When ShinyHunters breached companies' cloud computing providers, the conspirators sometimes also used the accounts to generate profit by crypto mining, while the cloud provider billed the use of computing power to the victim companies. PSR ¶ 27; Plea ¶ 9. In July 2020, Raoult sent messages on Discord about targeting Provider-1 accounts with the aim of both selling databases and using the cloud computing access for mining. SH-00118968 - 00118971. Raoult's personal involvement in profiting from hacking is discussed further below.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

From searches of Raoult's and his co-conspirators' devices and other electronic evidence collected during the investigation, the government has obtained limited snapshots of the ways that ShinyHunters profited, as described above. It is not possible to calculate the total profit from those limited snapshots. However, Bildstein estimated that the total profit from the ShinyHunters hacking activities was €3 million. SH-00119543.

C. The Hacking Scheme Harmed Dozens of Victim Companies and Hundreds of Millions of Their Customers

Raoult and his co-conspirators in the ShinyHunters group were extremely prolific in their hacking activities. Raoult conspired with Bildstein, El Ahmadi, and others from at least April 2020 to the end of June 2021. PSR ¶ 22. Between April 2020 and June 2021, ShinyHunters posted sales of hacked data from more than 60 companies. PSR ¶ 26; Plea ¶ 9. In just three months, between April and June 2020, Raoult and his co-conspirators in the ShinyHunters group hacked at least 17 companies.[2] The government's investigation focused on companies that had sensitive data, especially customer data, stolen and sold, but Provider-1 actually identified over 650 different user accounts that the conspirators breached between March 2020 and May 2020. SH-00002970, 00119847.

From victim companies, Raoult and his co-conspirators stole both the companies' own confidential and proprietary data, such as source code, and customer records, which included personally identifiable information and financial information. PSR ¶ 30; Plea ¶ 9. In total, the co-conspirators stole at least hundreds of millions of customer records. PSR ¶ 30; Plea ¶ 9. As shown in the RaidForums screenshot above, ShinyHunters frequently stole millions of customer records from a single company. SH-00002306. From Victim-4 alone, ShinyHunters stole 91 million customer records. From another

[2] *See* SH-00002469, 00002523, 00002615, 00002785, 00003095, 00003151, 00003165, 00003466, 00003865, 00005392, 00113117, 00116448, 00116452, 00116456, 00116458, 00119341.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

victim in the same RaidForums post, ShinyHunters reported having stolen 120 million customer records.

Stealing and selling customer records put these hundreds of millions of individual customers at risk of identity theft and financial loss. As ShinyHunters demonstrated by listing the number of stolen customer records in its sale offerings, buyers would value the stolen data based on the number of customers whose data could be used. Raoult understood that buyers of the stolen data sought to misuse customers' financial information, and yet he was eager to find those buyers. In August 2020, Raoult used his Sezyo#1234 account on Discord to make comments to a co-conspirator about the fact that people would be interested in buying stolen data from Victim-6, a U.S.-based diet and fitness company, so that they could steal credit card numbers:

Sezyo#1234	How many users on [Victim-6] do you have?	2020-08-14 13:09:28 UTC
Sezyo#1234	Go dump, I can find private individuals for you who would be willing to buy it to steal the credit card of an overweight family man	2020-08-14 13:10:59 UTC
Sezyo#1234	Nobody gives a damn as long as they have the money	2020-08-14 13:11:22 UTC
Sezyo#1234	Well, if there are 3m, that will sell for 3k	2020-08-14 13:11:34 UTC

SH-00116562 (translation from French); PSR ¶ 29. Customer records are valuable to criminals not just to be able to steal directly from their financial accounts but also to use stolen passwords to breach customers' other accounts and to use customers' information to target them with various frauds by phone or email. There is no way to know the total number of customers who suffered from financial loss or other types of identity theft as a result of the ShinyHunters hacking, nor is there any way to know the total loss to those customers. Given that ShinyHunters successfully sold vast numbers of customer records, however, it is likely that the harm to customers was significant.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Meanwhile, victim companies incurred substantial losses to respond to the hacks, especially conducting investigation and notifying affected customers. Victim companies also often suffer significant reputational damage and loss of business, which are real harms that are not accounted for in the loss calculations. As Victim-1 explained in its victim impact statement, this kind of hacking can damage the victim's brand and "threaten[s] to reduce customer trust in [a victim's] products and services, which cannot be remedied with any amount of damages."

Raoult admitted in his plea agreement that the total loss to victim companies is estimated to exceed $6 million. Plea ¶ 9. Seven victim companies have submitted loss calculations for which Raoult is responsible based on his participation in the conspiracy. SH-00003425, 00003864, 00114336, 00114344, 00114351, 00114356. From those submissions, there is a total of $5,058,419.73 in reported loss and restitution that Raoult owes:

Victim Number	**Loss/Restitution**
Provider-1	$501,808
Victim-7	$161,000
Victim-9	$1,000
Victim-10	$367,766.89
Victim-11	$350,000
Victim-12	$3,650,844.84
Victim-13	$26,000
TOTAL	**$5,058,419.73**

PSR ¶ 103.

The $5 million total of reported losses is a significant underestimate of the actual loss to victim companies, as numerous victim companies have not reported their losses. As noted above, hacking victims frequently suffer significant reputational damage and loss of business because of hacks, and they are concerned that further publicity will cause further harm. Although victim impact statements and restitution requests would not

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

result in public disclosure of the victims' names, many victims fear that the information will be identifiable as linked to them. This is especially true in a case like this, where ShinyHunters and a number of the individual breaches have already received substantial publicity. To protect their businesses from further harm, many hacking victims choose not to report their losses to the government and the Court. As Provider-1 noted in its victim impact statement, "Each of the 650+ victims [Provider-1] identified will have had their own incident response costs and downstream impact." But the known loss information is based on just seven companies reporting. Thus, the true total loss to victim companies is likely to be much higher than the $5 million in known loss.

Furthermore, many individuals suffered harm that is not accounted for in the reported company losses. As explained above, the financial loss and identify theft suffered by the millions of individual customers of victim companies is a separate harm that is not measurable. In addition, Provider-1's victim impact statement highlights the psychological impact on the hundreds of people whose accounts were breached.

D. Raoult Hacked For At Least Two Years

Raoult engaged in hacking for profit for at least two years, including the charged ShinyHunters hacking scheme and various other hacking activities. The evidence contains references to Raoult's hacking as early as 2018. After the charged ShinyHunters hacking activity, Raoult continued to hack through at least March 2022, shortly before his arrest in Morocco in May 2022.

Several references in the discovery for this case indicate that Raoult had been involved in hacking prior to participating in the ShinyHunters hacks. In a 2021 chat found on Raoult's phone, Raoult told his correspondent, "In 2018 I hacked [Victim in crypto industry] and exchanged their token in hitbtc the only platform that accepts this currency I had 200k but 10 btc still remaining . . . ." SH-00118807, chat-2.txt. In December 2019, Raoult told someone in Discord messages, "I want to hack," and Raoult further commented, "I wouldn't be able to start targeting crypto sites again like I did

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

before." SH-00118958 – 00118959 (translation from French); PSR ¶ 29. Thus, Raoult was not new to hacking in the spring of 2020.

Between April 2020 and June 2021, Raoult participated in the prolific ShinyHunters hacking conspiracy with Bildstein, El Ahmadi, and others. PSR ¶ 22. As described above, Raoult and his co-conspirators hacked at least 17 companies in just three months, between April 2020 and June 2020. As Provider-1 has flagged, the conspirators actually breached hundreds of accounts, but not all breaches yield valuable customer records to sell. This was a particularly active period for the ShinyHunters group, both for hacking and for posting sales of data from a large number of companies. Between July 2020 and at least June 2021, Raoult continued to hack with some of the same co-conspirators, including hacking companies through their employees' accounts at Provider-1. PSR ¶ 22; Plea ¶ 9. Raoult, El Ahmadi, and others continued to work together to target accounts at Provider-1, and the ShinyHunters profile continued to offer sales of the companies that Raoult and the others discussed hacking.

For instance, in the timeframe between July 2020 and June 2021, Discord messages indicate that Raoult continued to participate in hacking activities with El Ahmadi that targeted accounts at Provider-1. In March 2021, Raoult and a correspondent discussed setting up a Telegram channel with "abdel" because "He wants to prepare sawfish." SH-00118950 (translation from French).

Also, again in the timeframe between July 2020 and June 2021, Raoult engaged in extensive discussions about hacking collaboration with an individual using the Discord account Liebert#3914. The ShinyHunters account shinyhunters@xmpp.jp, which was used to coordinate sales of hacked data for Raoult and his co-conspirators, as discussed above, then had conversations with potential buyers about the same victim companies that Raoult and Liebert#3914 discussed.

Raoult, using his Discord account Sezyo#1234, had a variety of discussions with Liebert#3914 showing that they were still engaged in hacking companies through

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

accounts at Provider-1. For example, in March 2021, Liebert#3914 asked Raoult, "Can you check [Provider-1] tokens?" SH-00116859 (translation from French). In August 2020, Raoult told Liebert#3914, "send me the repositories." SH-00116565 (translation from French). In January 2021, Raoult told Liebert#3914, "Come on, we'll leak their repositories to create buzz." SH-00116638 (translation from French). As described above, companies' code stored with Provider-1 was kept in locations called "repositories." *See* PSR ¶ 12.

ShinyHunters offered sales of companies that Raoult and Liebert#3914 discussed breaching. For example, in August 2020, Raoult told Liebert#3914, "[Victim-6], if you manage to dump the customers, that will be a good haul for you." SH-00116552 (translation from French). Raoult continued with the conversation already quoted above, where he asked "How many users on [Victim-6] do you have?" and encouraged Liebert#3914 to "Go dump" so they could sell to a buyer who wanted to steal credit cards. SH-00116562 (translation from French); PSR ¶ 29. A week later, Shinyhunters@xmpp.jp told a correspondent that he had breached Victim-6 recently and told another correspondent that he would be offering Victim-6's database for sale. SH-00116287. Similarly, also in August 2020, Raoult asked Liebert#3914, "Did your cracker take care of the [Victim-5] hashes?" SH-00116571 (translation from French). This appears to refer to breaking the encryption protecting customer passwords that were stolen from Victim-5. Shinyhunters@xmpp.jp offered to sell the data from Victim-5 for $5,000. SH-00116287. Thus, after June 2020, Raoult continued to participate in the hacking activities that resulted in ShinyHunters sales.

ShinyHunters also continued to demonstrate prolific hacking activity for more than a year. In November 2020, shinyhunters@xmpp.jp told a potential buyer that he had about 100 databases available for purchase and sent another potential buyer a list of 16 specific databases available for purchase. SH-00116287. In March and April 2021, shinyhunters@xmpp.jp stated "I won't sell anymore, I found a more profitable way tbh"

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

and "ransom is profitable for me, otherwise I can put on auction." SH-00116287. In early May 2021, he bragged that he had extorted a particular victim for $1 million. SH-00116287. All of this shows that between July 2020 and June 2021, ShinyHunters continued to engage in extensive and damaging hacking activity, and Raoult continued to participate in hacking with ShinyHunters.

In March 2021, Raoult even described some of his ongoing hacking of companies through Provider-1 accounts to a contact who was not part of ShinyHunters. Raoult said "Im doing [Provider-1] phishing rn" and "Clone private repos and looking for interesting access point in it." SH-00118807, chat-2.txt. He sent an example of one of his phishing domains. Raoult explained that he was getting access credentials to cryptocurrency accounts by targeting victim companies in the cryptocurrency industry: "I have to find what [Provider-1] organizations are working in crypto then I target them." SH-00118807, chat-2.txt. As an example, Raoult said that he had hacked a cryptocurrency wallet company "[t]hrough their [Provider-1]" token the previous month and got $300,000 but he needed to wait until 2022 for the money to be unlocked. SH-00118807, chat-2.txt.

Shortly before Raoult's arrest in Morocco in May 2022, he was still actively engaged in hacking. One of Raoult's phones that was seized at the time of his arrest contained a lengthy group Telegram chat from March 2022 that was entitled "[Provider-1] | Sawfish" and contained thousands of messages that appear to be automated messages related to [Provider-1] phishing attempts. SH-00118805, chat-3.txt. One of the participants in the message chain was labeled "Telegram Bot Raw," confirming the impression that the automated-looking messages came from a bot, a software program that is coded to perform a repetitive task. In this case, the bot appears to have provided Raoult and his co-conspirators with information about the status of [Provider-1] phishing attempts. During just one week, from March 15 to March 22, 2022, this Telegram bot chat contained thousands of messages about [Provider-1] logins and two-factor

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

authentication successes. SH-00119560 - 00119561. There were over one thousand different email addresses and over one hundred passwords in the chats. SH-00119562, 00119564. Some of the email accounts were likely test accounts used by Raoult and his co-conspirators, but many of them were associated with government agencies, educational institutions, and major companies, indicating that they were probably phishing victims. Some typical messages looked like this:

```
----------------------------
From: 35287810358 Rezman
Timestamp: 3/17/2022 12:54:27 PM(UTC+0)
Source App: Telegram
Body:
+1 LOGIN [Provider-1]
# Email : [Victim email at major U.S. tech company]
# Username : [Redacted]
# Pass : [Redacted]
----------------------------
From: 35287810358 Rezman
Timestamp: 3/17/2022 12:54:28 PM(UTC+0)
Source App: Telegram
Body:
2FA SUCCESS SENT
# IP : 194.230.147.151
# Operateur : as6730 sunrise upc gmbh (CH)
----------------------------
```

SH-00118805, chat-3.txt.

During the same week, Raoult and co-conspirators exchanged messages in a separate Telegram chat thread confirming that they were working on breaching victim companies through their Provider-1 accounts. SH-00118805, chat-1.txt. Participants talked about having stolen 2 million emails from Provider-1, phishing Provider-1, using a bot, and downloading private repositories. SH-00119595, 00119672, 00119678-00119679, 00119686. Someone shared the URL for a phishing website. SH-00119837 – 00119838, SH-00119066 - 00119071. Raoult commented, "I want to pad my wallet," and a co-conspirator responded, "Thanks to the repository we're going to steal." SH-00119609 - 119610 (translation from French). Raoult announced:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

From: 1040916755 Mr. Mask (Sezyo)

Timestamp: 3/18/2022 1:36:24 AM(UTC+0)

Source App: pp: Telegram

Body:

la c vraiment Sawfish Rebirth

It's really Sawfish Rebirth

SH-00119715 (translation from French). Thus, two years after the earliest evidence of his participation in the ShinyHunters scheme and just two months before his arrest, Raoult was doing exactly the same sort of hacking that he had done with the ShinyHunters group.

E. Raoult Hacked for the Purpose of Profit

Personal profit motivated Raoult's hacking, as he expressed explicitly and also repeatedly demonstrated. In December 2019, Raoult explained to someone that he wanted to hack, sell databases, and become a millionaire:

Sezyo#1234	I could say that my goal is to be a millionaire before I turn 20, but it's all well and good to say that	2019-12-19 00:22:37 UTC
Sezyo#1234	I don't have any references except for shiny hunter	2019-12-19 00:23:16 UTC
[*13-line break*]		
Sezyo#1234	Anyway I want to hack and [vulgar]	2019-12-19 00:28:46 UTC
Sezyo#1234	I'm going to resell databases to Indians on the darknet	2019-12-19 00:31:12 UTC

SH-00118956 – 00118958 (translation from French); PSR ¶ 29.

In conversations with ShinyHunters co-conspirators and others, Raoult demonstrated his desire to profit from the sale of databases. In May 2020, Raoult asked Bildstein about how the sale of Victim-4's data was going, as described above. PSR ¶ 26; SH-00119339. Bildstein told French law enforcement that he shared the profits of their hacking with Raoult and stated that he gave Raoult about €100,000. PSR ¶ 28; SH-

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

00119519. Although it is appropriate to view comments from a fellow hacker critically, Bildstein provided a substantial amount of detail about the ShinyHunters scheme to law enforcement, and many details are corroborated by other evidence. As discussed above, Bildstein identified Raoult as the primary developer of the software code for the Sawfish hacking campaign, which is corroborated by the technical evidence and Raoult's own admissions. Bildstein's statements about sharing profits with Raoult are consistent with the other evidence that Raoult aimed to profit and wanted stolen data to be sold. Furthermore, it is not clear why Bildstein would have had any motive to lie about this. Comments from Bildstein are relevant and useful where, as here, they are consistent with other evidence and seem to contribute context to it.

Raoult was involved in numerous additional conversations that confirm his efforts to profit from data sales. PSR ¶ 29. In August 2020, Raoult discussed the potential for selling data from Victim-6 to buyers who wanted to steal credit cards, as quoted above. PSR ¶ 26; SH-00116562. In January 2021, Raoult complained about "the person who leaked [Victim-5] when I thought they were going to resell it, it seriously drives you crazy." SH-00116676 – 00116677 (translation from French); PSR ¶ 29. In July 2020, Raoult wrote, "we're going to do [Provider-1] spamming" and "I'm telling you bro, the SMTPs that we'll have and the databases we'll be able to crack, there will be stuff to resell, plus the [Cloud provider] mining." SH-00118968 – 00118971 (translation from French). In March 2021, while discussing his current hacking of companies in the cryptocurrency industry, Raoult offered to sell someone "300 Gb KYC documents" and said that he expected to get "maybe 100-200k" for them. SH-00118807, chat-2.txt. "KYC" is a common abbreviation for Know-Your-Customer, which refers to the information and documents that cryptocurrency and other financial businesses collect to verify customers' identities. Thus, Raoult was likely offering to sell a large database of identification documents. Taken together, these conversations leave no doubt that Raoult intended to profit from selling the data that he hacked.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

In addition to seeking to profit from hacking victims with valuable customer data that could be sold, Raoult targeted victims in the cryptocurrency industry that could provide access to funds. Sometimes Raoult accessed stolen funds directly, and sometimes Raoult sold access keys so that others could withdraw funds. PSR ¶ 27; Plea ¶ 9. For example, Raoult talked about a time that he and co-conspirators hacked a cryptocurrency exchange and got over $100,000:

Sezyo#1234	Remember, that's the method that I used to hack an exchanger	2020-07-19 03:01:17 UTC
Sezyo#1234	Where there was more than 100k where we split it three ways	2020-07-19 03:01:31 UTC

SH-00118961 (translation from French). In multiple conversations, Raoult talked about selling cryptocurrency access keys on darkweb marketplaces so that other criminals could withdraw stolen funds. For example, in the message below, Raoult showed that he had posted on RaidForums a sale of Binance access keys to a total of $637,000 in funds:

Sezyo#1234	https://raidforums.com/Thread-SELLING-160-Binance-API-keys-637k-USD-total-balance	2021-03-15 00:41:31 UTC
Sezyo#1234	I POSTED IT	2021-03-15 00:41:36 UTC

SH-00086481.

Indeed, Raoult made no secret of the fact that he would rather hack and steal money than do legitimate work:

Sezyo#1234	Today at 04:01 I don't know if I want a job that keeps me stable, that's not the question, but I prefer to hack a crypto exchange 😆	2020-07-21 02:07:30 UTC

SH-00118962 (translation from French).

There are indications that Raoult also lost a substantial amount of money related to cryptocurrency hacking when he tried to hide his control of the funds or pay other criminals to help with particular services. Bildstein reported that Raoult ended up being scammed out of a large amount of cryptocurrency from ShinyHunters crypto hacks when

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

he tried to anonymize it using a service that turned out to be a scam. SH-00119541. In another example, in March 2021, Raoult talked to someone about having sent him a total of about $14,000 that the person was supposed to use to help Raoult access cryptocurrency funds using stolen access keys, but it appears from the conversation that the person took the money without helping Raoult. SH-00118807, chat-2.txt.

Besides Raoult's various efforts to profit by stealing money and data from hacking victims, Raoult also obtained significant profits by selling his software code so that others could use it to conduct their own hacks. Raoult admits that he sold exploit kits to others. PSR ¶ 27; Plea ¶ 9. In December 2020, Raoult said that he had sold "a script to find SMTPs with git config," "I sold it to four people between 2k and 3k." SH-00116629 – 00116630 (translation from French). In March 2020, Raoult stated that he sells "one copy of my smtp cracker script" for "5k." SH-00118807, chat-2.txt. The best summary of Raoult's script sales appears to come from a message in April 2022:

> ---
> From: 1040916755 Mr. Mask (Sezyo) (owner)
> Timestamp: 4/6/2022 3:05:47 AM(UTC+0)
> Source App: Telegram
> Body:
> I was selling the script .git for 5k€, I sold maybe a dozen, and then I focused on cashing out BTC [Bitcoin Crypto Currency], I stopped selling stuff.
> ---
> From: 1040916755 Mr. Mask (Sezyo) (owner)
> Timestamp: 4/6/2022 3:06:07 AM(UTC+0)
> Source App: Telegram
> Body:
> And I leaked my stuff when I had too much money
> ---

SH-00118954. Selling the hacking script for €5,000, a dozen times, means that Raoult would have made €60,000 from the total sales. As Raoult admits, he made so much money from his hacking activities and sales of hacking scripts that there were times when he "had too much money."

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

F. Procedural History

On June 23, 2021, a grand jury indicted Raoult and co-defendants Bildstein and El Ahmadi for conspiracy to commit computer fraud and abuse, in violation of 18 U.S.C. §§ 371 and 3559(g)(1); conspiracy to commit wire fraud, in violation of 18 U.S.C. §§ 1349 and 3559(g)(1); four counts of wire fraud, in violation of 18 U.S.C. § 1343; and three counts of aggravated identity theft, in violation of 18 U.S.C. § 1028A(a). ECF No. 1.

The United States requested assistance from French law enforcement with investigating the defendants and other subjects located in France. In late May and early June 2022, investigators traveled to France to participate in French law enforcement's interviews of Bildstein, El Ahmadi, and other subjects. French law enforcement also seized electronic devices from Bildstein, El Ahmadi, and the other subjects, and they provided copies of certain contents to the U.S. investigators. French law enforcement had also provided copies of certain contents from devices belonging to Bildstein in December 2021. There was no interview of Raoult during the May 2022 operation, because Raoult was not in France. Although France provided this requested assistance in the U.S. investigation, France will not extradite its own citizens. As the French Ministry of Justice has explained, "the fact that the wanted individual is a French national constitutes an insuperable obstacle to his/her removal." Letter from the French Ministry of Justice, *United States v. Ghislaine Maxwell*, No. 1:20-cr-330, ECF No. 165-1 (S.D.N.Y. Mar. 9, 2021).

Investigators located Raoult in Morocco, where he had apparently been living for several months, and Moroccan authorities arrested him at the request of U.S. authorities on May 31, 2022. PSR ¶ 4. Raoult fought extradition to the United States in multiple ways. The month before he was extradited, he tried to block the extradition by filing a petition with the U.N. Committee Against Torture, claiming that the potential sentence in the United States would constitute degrading or inhumane treatment. *See Counsel for*

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Alleged Member of ShinyHunters Tries a Legal 'Hail Mary' Play to Block Extradition, DataBreaches, December 28, 2022, https://www.databreaches.net/counsel-for-alleged-member-of-shinyhunters-tries-a-legal-hail-mary-play-to-block-extradition/. Raoult ended up remaining in Moroccan custody pending extradition for approximately eight months.

While Raoult fought against extradition, he proclaimed his innocence to the French media. He claimed that he was actually a victim of identity theft and that his identity had been stolen so that he could be used as a scapegoat for cybercrime. *See* Exhibit 1, Translation of French Article from L'Obs; *Je me refuse a croire que la France m'a abandonne au sort de la justice americaine*, L'Obs, October 3, 2022 (SH-00116470). He also complained to the media about the prison conditions in Morocco, although his description of conditions at that time was somewhat less extreme than his recent description to Probation. *Id.* Through his attorneys, Raoult also described his experience in Moroccan prison as part of his attempt to achieve temporary release from U.S. custody, complaining, among other things, that he ate "off a plate on the ground." ECF No. 34 at 1-2. Some of the aspects that Raoult has described are cultural differences, such as using hands to eat off plates on the floor and using squat toilets on the ground with water rather than toilet paper, but it is understandable that they contributed to the shock and discomfort of the experience for a European.

On January 25, 2023, Moroccan authorities turned Raoult over to the custody of U.S. law enforcement in Morocco. PSR ¶ 5. Moroccan authorities also turned over devices that had been seized from Raoult at the time of his arrest, as well as Raoult's personal property, which U.S. law enforcement has returned to Raoult's parents. Raoult's personal belongings included, among other things, Gucci luggage, a Dior bag, several Gucci sweaters, and Gucci pants. *See, e.g.*, SH-00113416.

Raoult made his initial appearance in Seattle on January 27, 2023. PSR ¶ 5. On September 27, 2023, Raoult pled guilty to conspiracy to commit wire fraud, in violation

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

of 18 U.S.C. §§ 1349 and 3559(g)(1), and aggravated identity theft, in violation of 18 U.S.C. § 1028A(a). ECF No. 50.

II. SENTENCING GUIDELINES CALCULATIONS

A. Offense Level

The government agrees with the sentencing guideline calculations in the PSR. *See* PSR ¶¶ 38-52. For Count 2, the base offense level is 7. U.S.S.G §§ 2X1.1(a), 2B1.1(a)(1). Eighteen levels are added for a loss of more than $3.5 million. U.S.S.G. § 2B1.1(b)(1)(J). Raoult also receives three 2-point enhancements because the offense involved 10 or more victims, the offense involved stealing and selling stolen property, and the offense both involved sophisticated means and a substantial part of it was committed from outside of the United States. U.S.S.G. §§ 2B1.1(b)(2)(A), (b)(4), and (b)(10). There is also a 2-point adjustment for knowingly falsely registering a domain name. U.S.S.G. § 3C1.4. Taking into account a 3-point reduction for Acceptance of Responsibility and a 2-point reduction based on the Zero-Point Offender Amendment, the total offense level for Count 2 is 28. *See* U.S.S.G. §§ 3E1.1, 4C1.1. For Count 8, there is no calculation of offense level because the guideline term is the mandatory consecutive 2-year term required by statute. U.S.S.G. § 2B16.

B. Criminal History Category

Raoult's criminal history score is zero and his Criminal History Category is I. PSR ¶¶ 53-58.

C. Guidelines Range

For Count 2, the guideline sentencing range based on a total offense level of 28 and a Criminal History Category of I is 78 to 97 months of imprisonment. PSR ¶ 91. For Count 8, the guideline sentencing range is 24 months of imprisonment, which must be consecutive to the term on Count 2. PSR ¶ 91. Therefore, the guideline imprisonment range for the total sentence on both counts is 102 to 121 months of imprisonment. PSR ¶ 91.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

III. FACTORS RELATED TO SENTENCING RECOMMENDATION

For over two years, Raoult participated in extensive computer hacking that caused millions of dollars in losses to victim companies and unmeasurable additional losses to hundreds of millions of individuals whose data was sold to other criminals. Raoult did all of this for the sake of personal profit, despite knowing that he and his co-conspirators were providing the tools for other criminals to steal from innocent individual victims. Therefore, a substantial sentence of imprisonment is important to achieve deterrence and protect the public. The most analogous case in this district is the FIN7 prosecution, which concerned another for-profit international hacking conspiracy and resulted in sentences between five and ten years of imprisonment, as discussed further below.

The United States respectfully requests a below-guideline sentence of 72 months of imprisonment, as well as a 3-year term of supervised release and restitution in the amount of $5,058,419.73. The government has reached this sentencing recommendation after careful consideration of both the extremely serious nature of Raoult's offense and the mitigating factors in his case. Under the plea agreement, the government may recommend a sentence up to 87 months. That already reflected the government's evaluation of certain mitigating factors. However, based on additional mitigating information that has emerged in the PSR process, the government believes that a 72-month sentence would be appropriate. This accounts for Raoult's extremely harmful conduct as a participant in the for-profit international hacking conspiracy and his lengthy involvement in hacking, and it also accounts for his challenging family circumstances and time spent in a foreign prison.

A. Nature and Circumstances, and Seriousness of the Offense

Raoult's offense was extremely serious and caused enormous harm. He and his co-conspirators in the ShinyHunters hacking group hacked and advertised stolen data from over 60 victim companies. In just three months of particularly prolific hacking activity, between April 2020 and June 2020, Raoult and his co-conspirators hacked at

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

least 17 companies. They actually breached hundreds of companies but may not have found data that was as valuable for sale. Based on just seven victim companies reporting, this caused an actual loss of over $5 million to the companies.

The $5 million loss figure is a dramatic underestimate of the true harm that Raoult and his co-conspirators caused. This figure excludes the loss suffered by the numerous victim companies who felt that they could not report their losses to this Court without risking further harm to their businesses. It also excludes many real harms that companies suffer as a result of hacking but are not included in the loss calculation for guidelines purposes, such as reputational damage, loss of customers, and litigation costs.

Most importantly, the $5 million loss figure does not account for the losses that the hundreds of millions of individual consumers suffered as a result of having their data hacked. As Raoult well understood, the stolen customer data was valuable because buyers could use it to steal from the customers. It is impossible to measure the total loss that individual consumers suffered from stolen credit card numbers, other identity theft, and other types of fraud, but it was likely very substantial given the number of records stolen.

Raoult played a key role in the conspiracy that caused this harm. He developed a substantial portion of the software code and phishing websites that he and his co-conspirators used to hack companies through their employees' accounts at Provider-1, and he personally participated in hacking companies. The ShinyHunters hackers, including Raoult personally, also committed identity theft to use employees' passwords and user information to breach their employers' companies.

Raoult's motive was pure greed. He wanted to become a millionaire by selling hacked data. He wanted to steal people's cryptocurrency. He even sold his hacking tools so that he could profit while other hackers attacked additional victims. Although Raoult's father told Probation that he thought Raoult was living like a student, in fact Raoult was arrested with expensive designer luggage and designer clothing. Raoult's

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

electronic messages described above show that Raoult made at least about $100,000 from just the sales of his hacking scripts and the hack of one cryptocurrency exchange. Raoult explained his offense to Probation as related to being "locked in my room all the time during the pandemic," PSR ¶ 36, but actually Raoult was engaged in hacking and aimed to become a millionaire from selling hacked data long before the pandemic began. Raoult was happy to profit from hacking while knowing that buyers would use the hacked data to steal from the millions of individual victims: "Go dump, I can find private individuals for you who would be willing to buy it to steal the credit card of an overweight family man." SH-00116562 (translation from French).

Playing a substantial role in such extensive hacking, causing such significant harm to individual consumers and companies, and doing it for the sake of personal profit all support the 72-month sentence that the government is requesting.

B. History and Characteristics of the Defendant

Raoult's personal history includes both aggravating and mitigating factors. The length of time that Raoult was involved in hacking is a significant aggravating factor. The government possesses detailed evidence of his extensive involvement in hacking between April 2020 and March 2022, and Raoult also made concrete references to his hacking activities as far back as 2018. Thus, Raoult was actively engaged in hacking for at least two years and probably more than three years. Raoult's participation in the ShinyHunters scheme was consistent with a course of criminal conduct, rather than being an aberration. His Criminal History Category of I does not account for the fact that he was involved in other serious hacking activity and was simply not caught.

Hacking for profit over those years is also an aggravating factor, especially given that Raoult did not need the money. He apparently used it for luxury goods such as designer clothing, among other things. He even told someone that he sometimes "had too much money" from his hacking. SH-00118954.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Along with these aggravating factors, there are mitigating factors in Raoult's background. Like many defendants before this Court, he has had family members who experienced addiction, were victims of violent crime, or had serious medical challenges. Like many defendants before this Court, he is relatively young. For a young person to have such experiences could certainly contribute to unsettling him, although they are far from excusing or justifying actions that wreaked such havoc on so many innocent victims. Raoult also spent eight months isolated in prison in a foreign country while fighting extradition and since then has spent almost a year in prison in the United States, both times far from home and family.

The 72-month sentence that the government recommends reflects an effort to balance the aggravating and mitigating factors in this case. A low-end guideline sentence would be 102 months. In addition, the guideline range reflects a very conservative measure of loss that does not account for much of the harm that Raoult and his co-conspirators caused. Therefore, the government believes that a 72-month sentence is appropriate to account meaningfully for the mitigating factors in Raoult's history while still addressing the magnitude of Raoult's offense and the other sentencing factors, such as the need for deterrence and protecting the public, as discussed below.

C. Need to Promote Respect for the Law, Provide Just Punishment for the Offense, and Afford Adequate Deterrence

Because of the significant harm that Raoult caused, promoting respect for the law, providing just punishment, and deterring such conduct are important. Both specific deterrence and general deterrence are relevant considerations in this case.

Raoult's history suggests that meaningful consequences are necessary to deter his hacking activity. He hacked for profit for at least two years. He told someone that he preferred hacking over having a stable job. Given that a limited review of his phones revealed evidence of active hacking activity in March 2022, just two months before his arrest, it appears that he stopped hacking only because he was imprisoned for this case.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

After he was caught and had been detained for several months, he was still proclaiming his innocence to the media and insisting that he was a victim of identity theft. This history shows that serious intervention is required to stop Raoult's hacking. Furthermore, when Raoult finishes his prison sentence, he will presumably return to France, where he knows that the United States has no power to extradite him for any future hacking of U.S. victims. This makes it especially vital that Raoult's sentence achieve effective deterrence.

In cases involving foreign hackers like Raoult, general deterrence takes on unusual importance. As news reports demonstrate to all of us on a daily basis, computer hacking has become a monstrous problem for U.S. security, the economy, and all of the U.S. residents whose financial information and personal lives are constantly at risk of exposure. Statistics can help to illustrate the breadth of the problem, although they cannot convey its full extent. For example, just payments of ransoms by hacking victims who were breached by ransomware was estimated to cost a total of $20 billion in 2021. Cybersecurity Ventures, *Global Ransomware Damage Costs Predicted to Exceed $265 Billion by 2031*, https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/. That $20 billion total does not include other types of harm from hacking, such as the many data breach victims who must pay large costs for investigation and victim notification. A recent study by IBM found that the average cost for a single company experiencing a data breach in 2023 was $4.45 million. IBM, *Cost of a Data Breach Report 2023*, https://www.ibm.com/reports/data-breach. In addition, all companies, government agencies, and other institutions must bear substantial cybersecurity costs to try to protect themselves against the constant risk of being hacked.

Individuals are the real victims of this explosion in computer hacking. Consumers are hurt directly, as their personal and financial information is often the target of the hacking. As demonstrated by this case, a breach of a single victim company may expose

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

personal information for millions or even a hundred million individuals. As occurred in this case, hackers seek that information in order to sell it to other criminals who want to steal people's credit cards, commit other types of identity theft, and use their information to target them for various frauds. Consumers are also hurt indirectly as they must ultimately shoulder the costs that companies and governments bear, both the direct losses from data breaches and the ongoing large expenses for cybersecurity to try to prevent more data breaches. As Attorney General Garland has summarized, "Cybercrime is a serious threat to the country: to our personal safety, to the health of our economy, and to our national security." U.S. Department of Justice, *Comprehensive Cyber Review July 2022* at 6, https://www.justice.gov/dag/page/file/1520341/download.

Hacking by foreign cybercriminals is a particularly huge problem, both because such foreign hackers cause a vast amount of damage to the U.S. and its people, and because it is so much more difficult for U.S. law enforcement to hold foreign hackers accountable. In some cases, like Raoult's, holding a foreign hacker accountable just involves a much greater expenditure of law enforcement resources, including seeking international assistance and dealing with a lengthy extradition process. But in many cases, it is impossible for U.S. law enforcement to bring foreign hackers to justice. For example, many countries will not extradite people to the United States at all or will not extradite their own citizens. This prosecution is a good example. Although there are three charged defendants, the government has been able to arrest only Raoult. There are many cases that are worse, where the U.S. government has been unable to apprehend anybody.

The difficulty of holding foreign hackers accountable for their crimes makes it especially vital to achieve general deterrence through meaningful sentences when foreign hackers do face the U.S. justice system. It would not be appropriate, as Probation suggests, to consider a lesser sentence for Raoult because his co-defendants will potentially face little or no penalty for their role in the crime. The logical outcome of that

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

reasoning would be that U.S. courts would never hold foreign hackers accountable because so many other foreign hackers cannot be held accountable. The inability to catch all criminals does not justify failing to punish and deter those who are caught. On the contrary, when it is challenging to catch the perpetrators, it is particularly vital for those who are caught to receive substantial prison sentences so that other would-be criminals must weigh the risk of such punishment.

Unfortunately, Raoult's relative youth is also a common characteristic for many successful hackers and hacking groups, who nevertheless cause tremendous damage. As with other crimes that this Court frequently sees, such as narcotics and violent crime, many of the defendants are in their twenties. Just as in those other cases, giving Raoult a substantial discount on his sentence because of his youth would fail to achieve adequate deterrence or protect the public.

Both to deter Raoult personally and to deter the swarms of foreign hackers eager to victimize Americans every day, a 72-month sentence is appropriate.

D. Need to Protect the Public from Further Crimes

The need to protect the public from further crimes also supports the requested 72-month sentence. As noted above, when Raoult finishes his prison term, he intends to return to France, where his co-defendants still reside and from which the United States would not be able to extradite him. Especially in light of Raoult's history of hacking for years, a significant prison sentence is necessary to disrupt Raoult's hacking and ensure that he cannot commit further breaches during that period of incarceration. That substantial period away from hacking and away from the people Raoult hacked with in the past is also important to achieve adequate deterrence and thereby protect the public from further hacking by Raoult when he leaves prison and is no longer subject to the U.S. justice system.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

E. Need to Avoid Unwarranted Sentence Disparity Among Similarly Situated Defendants

A 72-month sentence would not create any unwarranted sentencing disparities and would be consistent with the limited comparators in this district. Raoult is the only defendant in custody for this case. Due to the difficulty of identifying and apprehending many hackers, there have not been many recent sentencings in this district for defendants convicted of hacking activity that is comparable in volume and harm to Raoult's, but there is one comparable case.

The analogous recent case in this district is the FIN7 prosecution, which involved three defendants who had worked with over 70 other co-conspirators in an international conspiracy to breach over 100 companies and steal over 20 million customer credit and debit card numbers, which they sold for profit. *See* Gov. Sentencing Mem., *United States v. Hladyr*, No. 2:17-cr-00276-RSM, ECF No. 85 (W.D. Wash. Apr. 9, 2021); Gov. Sentencing Mem., *United States v. Kolpakov*, No. 2:18-cr-00159-RSM, ECF No. 59 (W.D. Wash. June 17, 2021); Gov. Sentencing Mem., *United States v. Iarmak*, No. 2:19-cr-00257-RSM, ECF No. 54 (W.D. Wash. March 29, 2022). The loss to victims was over $100 million. None of the three defendants was among the top-level leaders of the conspiracy, although two were managers. The three defendants, who qualified for departures from their sentencing guidelines imprisonment ranges, received sentences of ten years, seven years, and five years in prison.

Raoult is similarly culpable to the FIN7 defendants because both Raoult and the FIN7 defendants engaged in extensive hacking for personal profit, as members of for-profit international hacking conspiracies that harmed many companies and millions of their customers. The greater known loss amount in FIN7 is not a good measure of those defendants' relative culpability because of other differences between the two cases. First, while the loss to victims in FIN7 was over $100 million, the total loss to customers in this case is not available or measurable. Given the more than 60 companies breached and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

hundreds of millions of customers' records stolen, this case is much more similar to FIN7 than the known $5 million loss from a few companies conveys. Second, Raoult was one of a few key participants in the charged conspiracy, whereas the three FIN7 defendants worked with over 70 other perpetrators to achieve the total loss and were not top-level leaders of that conspiracy. Finally, another important consideration is that Raoult has not cooperated to try to stop or mitigate the damage from ongoing hacking activities. Taking all of these factors together, Raoult's conduct warrants a sentence similar to the FIN7 defendants, and it is because of the mitigating personal factors that the government recommends a 6-year sentence, toward the low end of the range that the FIN7 defendants received.

Another recent hacking case in this district is *United States v. Thompson*, involving a breach of customer records for over 100 million people, but that case is quite different from Raoult's case in important respects. *See* Gov. Sentencing Mem., *United States v. Thompson*, No. 2:19-cr-00159-RSL, ECF No. 377 (W.D Wash. Sept. 27, 2022). Thompson was not acting as part of an international conspiracy aimed at profiting while harming vast numbers of companies and people. Furthermore, there was no evidence that Thompson had sold or used the data that she hacked. Taking into account medical concerns related to imprisonment, the Court sentenced Thompson to Time Served and 5 years of probation. Because Raoult participated in a prolific for-profit conspiracy, his case is not comparable to Thompson's at all.

Like the FIN7 defendants, Raoult was a member of an international hacking conspiracy that caused substantial harm to numerous victim companies and their millions of customers for the sake of personal profit. Like the FIN7 defendants, Raoult should receive a substantial prison sentence.

//

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

IV. CONCLUSION

The government requests a sentence of 72 months in prison and $5,058,419.73 in restitution to address the millions of dollars in harm that Raoult caused to victim companies and immeasurable harm that he caused to hundreds of millions of individuals, all for the purpose of personal financial gain. This sentence is important to deter and protect the public from Raoult, who hacked for profit for at least two years, and is also necessary to deter the other foreign hackers who present a constant danger to this country, its economy, and its people.

DATED this 2nd day of January, 2024.

Respectfully submitted,

SARAH Y. VOGEL
Attorney for the United States, Acting under Authority Conferred by 28 U.S.C. § 515

s/ Miriam R. Hinman
MIRIAM R. HINMAN
Assistant United States Attorney
United States Attorney's Office
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
Phone: 206-553-7970
Fax: 206-553-4440